



UNITED STATES PATENT AND TRADEMARK OFFICE

Handwritten signature

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/637,229	08/11/2000	Cetin K. Koc	245-55512	7362
24197	7590	09/12/2006		
KLARQUIST SPARKMAN, LLP 121 SW SALMON STREET SUITE 1600 PORTLAND, OR 97204			EXAMINER LAFORGIA, CHRISTIAN A	
			ART UNIT 2131	PAPER NUMBER

DATE MAILED: 09/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	09/637,229		KOC ET AL.	
	Examiner		Art Unit	
	Christian La Forgia		2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 June 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 6-11, 16-18 and 22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 6-11, 16-18 and 22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 15 June 2006 has been entered.
2. Claims 6-11, 16-18, and 22 have been presented for examination.
3. Claims 1-5, 12-15, and 19-21 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments with respect to claims 6-11, 16-18, and 22 have been considered but are moot in view of the new ground(s) of rejection.
5. See further rejections that follow.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claim 22 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. The Examiner cannot find any discussion or illustration of a third and fourth processing unit in the

Art Unit: 2131

specification and drawings, respectively. The Applicant is required to show specifically where the third and fourth processing units are discussed to overcome this rejection.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

9. Claims 6-11 and 16-18 are rejected under 35 U.S.C. 102(a) as being anticipated by U.S. Patent No. 6,035,317 to Guy, hereinafter Guy.

10. As per claims 6 and 16, Guy discloses a cryptographic processor, comprising:

inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field (column 1, lines 17-22, column 1, lines 36-51, column 7, lines 35-38); and

a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including a first processing unit and a second processing unit (Figures 1 and 3 [blocks 19, 20]) configured to determine a Montgomery product of the cryptographic parameters (column 1, lines 7-22), the first processing unit and the second processing unit configured to receive a first bit and a second bit corresponding to the first parameter, respectively, and partial words of the second parameter (column 4, line 9 to column 5, line 36, column 7, line 33 to column 8, line 45, column 17, line 47 to column 18, line 50, column 20, lines 1-67, column 23, lines 8-67).

Art Unit: 2131

11. Regarding claim 7, Guy discloses wherein at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit (column 1, lines 7-22, column 4, line 9 to column 5, line 36, column 7, line 33 to column 8, line 45, column 17, line 47 to column 18, line 50, column 20, lines 1-67, column 23, lines 8-67).

12. Regarding claim 8, Guy discloses a field-representation-select input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with $GF(p)$ or $GF(2^m)$ arithmetic (column 1, lines 7-22).

13. With regards to claims 9 and 17, Guy teaches wherein the arithmetic operation selectable with the field-type input is field addition (column 6, lines 8-17, column 6, lines 46-53).

14. With regards to claim 10, Guy discloses a dual-field adder in communication with the field-type input (column 6, lines 8-17, column 6, lines 46-53).

15. Concerning claim 11, Guy teaches wherein the first and second cryptographic parameters are represented as m bits and e words of word length, wherein $\lceil (m + 1) / w \rceil$ (column 1, lines 30-43).

Art Unit: 2131

16. With regards to claim 18, Guy discloses a computer-readable medium containing instructions for executing the method of claim 17 (Figure 2 [block 3], column 8, line 60 to column 9, line 3).

Claim Rejections - 35 USC § 103

17. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

18. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Guy.

19. Regarding claim 22, Guy does not disclose the multiplication module further comprise a third processing unit and a fourth processing unit configured to receive a third bit and a fourth bit, respectively, corresponding to the first parameter and partial words of the second parameter.

20. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the multiplication module further comprise a third processing unit and a fourth processing unit configured to receive a third bit and a fourth bit, respectively, corresponding to the first parameter and partial words of the second parameter, since it has been held that it only requires routine skill in the art to merely duplicate a the first and second processing units thereby creating third and fourth processing units, especially since Guy discloses at column 1, lines 7-15 that by operating multiplication circuits in parallel improves the performance of modular operations according to the Montgomery method. See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Art Unit: 2131

22. The following patents are cited to further show the state of the art with respect to related applications, such as:

United States Patent No. 7,046,800 to Tenca et al., which is cited to show a commonly owned scalable Montgomery multiplication patent.

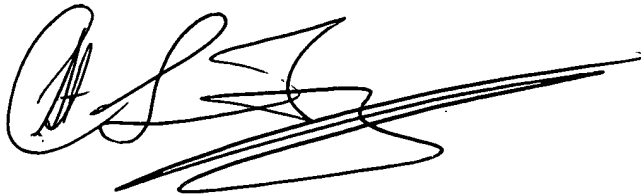
23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571) 272-3792.

The examiner can normally be reached on Mon-Thurs 7-5.

24. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

A handwritten signature in black ink, appearing to read 'CLF', with a long, sweeping horizontal stroke extending to the right.

clf